Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A system for presentation integrity, comprising:
an encrypter to encrypt formatting data associated with information content data; and
a formatter to decrypt the encrypted formatting data and to format the information content data in a predetermined format based on the decrypted formatting data.

[c2] 2. The system of claim 1, further comprising a plurality of formatters, each to decrypt the encrypted formatting data and to format the information content data in the predetermined format based on the decrypted formatting data.

[c3] 3. The system of claim 1, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

[c4] 4. The system of claim 1, wherein the formatter decrypts

the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assigned to a different copy of the information content data.

[c5] 5. The system of claim 1, further comprising an output device to present the information content data in the predetermined format.

[c6] 6. The system of claim 5, wherein the output device comprises at least one of a display and a printer.

[c7] 7. The system of claim 1, further comprising at least one of a computer and a media player to present the information content data in the predetermined format, wherein the formatter is embodied in the at least one of the computer or the media player.

[c8] 8. The system of claim 1, wherein the formatter decrypts the formatting data in response to a valid key.

[c9] 9. The system of claim 8, wherein the formatting data is encryptable and decryptable by a common key.

[c10] 10. The system of claim 8, wherein the formatting data is encryptable and decryptable by different keys.

[c11] 11. The system of claim 1, wherein the information content data is encryptable by the encrypter.

[c12] 12. The system of claim 11, wherein the information content data and the formatting data are decryptable in response to a valid key.

[c13] 13. The system of claim 11, wherein the information content data and the formatting data are each decryptable in response to different keys.

[c14] 14. The system of claim 11, wherein the information content data and the formatting data are encryptable in response to different keys and are decryptable in response to keys that are each different from the keys used to respectively encrypt the information content data and the formatting data.

[c15] 15. The system of claim 1, wherein the encrypter encrypts the formatting data into an encrypted style sheet language transformation (SLT).

[c16] 16. The system of claim 15, wherein the SLT is an extensible style language transformation (XSLT).

[c17] 17. The system of claim 15, wherein the formatter decrypts the encrypted SLT and transforms the information content data into a hypertext markup language (HTML) having the predetermined format in response to a valid password.

[c18] 18. The system of claim 17, further comprising a browser to receive the information content data in HTML and to present the information content data in the predetermined format.

[c19] 19. The system of claim 1, wherein the encrypter encrypts the information content data into an encrypted markup language (ML) and encrypts the formatting data into an encrypted style sheet transformation (SLT).

[c20] 20. The system of claim 19, further comprising an information broker to transmit the information content data in the encrypted ML and the formatting data in the encrypted SLT to the formatter, wherein the formatter transforms the encrypted ML into an HTML format based on the SLT in response to the formatter receiving a valid password.

[c21] 21. A system for presentation integrity, comprising:
a formatter to decrypt encrypted formatting data associated with information content data and to format the information content data into a predetermined format based on the decrypted formatting data; and
a device to present the information content data in the predetermined format.

[c22] 22. The system of claim 21, further comprising a plural-

ity of formatters, each to decrypt the encrypted formatting data and to format the information content data in the predetermined format based on the decrypted formatting data.

[c23] 23. The system of claim 21, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

[c24] 24. The system of claim 23, wherein each predetermined format provides a different version of the information content data for presentation.

[c25] 25. The system of claim 23, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

[c26] 26. The system of claim 21, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

[c27] 27. The system of claim 21, further comprising at least one of a computer and a media player to form the information content data in the predetermined format, wherein the formatter is embodied in the at least one of the computer or the media player.

[c28] 28. The system of claim 21, wherein the formatter is adapted to be included in a vehicle.

[c29] 29. The system of claim 28, wherein the vehicle comprises one of an aerospace vehicle, a watercraft and a terrestrial vehicle.

[c30] 30. The system of claim 21, further comprising at least one of an aerospace communication channel and a terrestrial communication channel, wherein the formatter receives information content data and encrypted formatting data via at least one of the aerospace communication channel and the terrestrial communication channel.

[c31] 31. The system of claim 21, wherein the formatter de-

crypts the information content data, if encrypted.

[c32] 32. The system of claim 21, wherein the formatter decrypts the formatting data and the information content data, if encrypted, in response to a valid key.

[c33] 33. The system of claim 21, wherein the formatter decrypts each of the formatting data and the information content data, if encrypted, in response to different keys.

[c34] 34. A system for presentation integrity, comprising:
an encrypter to encrypt formatting data associated with information content data; and
a decrypter to decrypt the formatting data; and
a formatter to format the information content data in a predetermined format based on the decrypted formatting data.

[c35] 35. The system of claim 34, wherein the decrypter decrypts the formatting data to provide a selected one of a plurality of predetermined formats when the decrypted formatting data is applied to the information content data, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide the selected one of the predetermined formats in response to applying the key associated with the selected predetermined format to the decrypter.

[c36] 36. The system of claim 34, wherein the decrypter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

[c37] 37. The data processing device of claim 34, wherein the formatting data is encryptable into an encrypted SLT.

[c38] 38. The system of claim 37, wherein the decrypter decrypts the encrypted SLT and transforms the information content data into a hypertext markup language (HTML) having the predetermined format in response to a valid password.

[c39] 39. The system of claim 38, further comprising a browser to receive the transformed information content data in HTML and to form the information content data in the predetermined format.

[c40] 40. A system for presentation integrity, comprising:
an encrypter to encrypt information content data and formatting data associated with the information content data;
an information broker to transmit the encrypted information content data and the encrypted formatting data to a client in response to an information request;

a formatter to decrypt the information content data and the formatting data and to format the decrypted information content data in a predetermined format based on the decrypted formatting data; and
a browser to present the information content data in the predetermined format.

[c41] 41. The system of claim 40, further comprising a plurality of clients, each client including a formatter to decrypt the information content data and the formatting data and to format the decrypted information content data in the predetermined format on each client based on the decrypted formatting data .

[c42] 42. The system of claim 41, wherein at least one client is adapted to be included in a vehicle.

[c43] 43. The system of claim 42, wherein the vehicle is one of an aerospace vehicle, a watercraft and a terrestrial vehicle.

[c44] 44. The system of claim 40, further comprising at least one of an aerospace communication channel and a terrestrial communication channel, wherein the formatter receives information content data and encrypted formatting data via at least one of the aerospace communication channel and the terrestrial communication channel.

[c45] 45. The system of claim 40, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

[c46] 46. The system of claim 40, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

[c47] 47. The system of claim 40, wherein the information broker comprises one of a buffer and a storage device.

[c48] 48. A device to process data, comprising:
an encrypter to encrypt formatting data associated with information content data; and
an information broker to transmit the encrypted formatting data and the associated information content data to a requestor in response to a request.

[c49] 49. The device of claim 48, wherein the encrypter en-

crypts the information content data.

[c50] 50. The device of claim 49, wherein the information content data is encryptable into an encrypted markup language (ML) format.

[c51] 51. The device of claim 50, wherein the formatting data is encryptable into a encrypted style sheet language transformation (SLT) format.

[c52] 52. The device of claim 48, wherein the encrypter encrypts the formatting data in response to a selected key.

[c53] 53. The device of claim 52, wherein the selected key is a different key from a key used to decrypt the encrypted formatting data.

[c54] 54. The device of claim 48, wherein the information broker comprises one of a buffer and a storage device.

[c55] 55. A device to process data, comprising:
a formatter to decrypt encrypted formatting data associated with information content data and to format the information content data into a predetermined format based on the decrypted formatting data; and
an output device to present the information content data in the predetermined format.

[c56] 56. The device of claim 55, wherein the formatter for-

mats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

[c57] 57. The device of claim 56, wherein each predetermined format provides a different version of the information content data for presentation.

[c58] 58. The device of claim 56, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of a motion picture, an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

[c59] 59. The device of claim 55, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

[c60] 60. The device of claim 55, further comprising at least one of a computer and a media player to form the information content data in the predetermined format, wherein the formatter is embodied in the computer or the media player.

[c61] 61. The device of claim 55, wherein the formatter transforms the information content data into a HTML format in response to a valid password, and wherein the device further comprises a browser to form the information content data in the predetermined format.

[c62] 62. An electronically-readable medium having thereon data structures, comprising:
information content data; and
formatting data applicable to the information content data to form the information content data in a predetermined format, wherein the formatting data is encrypted and is decryptable by a data processing device.

[c63] 63. The medium of claim 62, wherein the encrypted formatting data is decryptable by a selected key associated with a unique copy of the information content data.

[c64] 64. The medium of claim 62, wherein the encrypted formatting data is decryptable by each of a plurality of keys, each key being associated with a different format to

present the information content data based on decryption of the formatting data.

[c65] 65. The medium of claim 62, wherein the information content is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the data processing device.

[c66] 66. The medium of claim 62, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

[c67] 67. The medium of claim 62, wherein the formatting data is decryptable to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

[c68] 68. The medium of claim 62, wherein the information content is encrypted.

[c69] 69. The medium of claim 68, wherein the information content and the formatting data are decryptable in response to a valid key.

[c70] 70. The medium of claim 68, wherein the information content and the formatting data are each decryptable in response to different keys.

[c71] 71. The medium of claim 62, further comprising a marking to identify an authorized user of each copy of the information content data and encrypted formatting data.

[c72] 72. The medium of claim 71, wherein the marking is formed by one of a public key signature, steganography or watermarking to identify the authorized user of each copy.

[c73] 73. A method for presentation integrity, comprising:
decrypting encrypted formatting data associated with information content data; and
formatting the associated information content data in a predetermined format based on the decrypted formatting data.

[c74] 74. The method of claim 73, further comprising prevent-

ing the associated information content data from being formatted other than in the predetermined format.

[c75] 75. The method of claim 73, further comprising sending the encrypted formatting data and the information content data to a plurality of clients, wherein the information content data is formatted in the predetermined format at each client.

[c76] 76. The method of claim 73, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

[c77] 77. The method of claim 76, further comprising formatting the information content data into different versions for different audiences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

[c78] 78. The method of claim 73, wherein the encrypted for-

matting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

[c79] 79. The method of claim 73, wherein the encrypted formatting data is decryptable in response to a valid key.

[c80] 80. The method of claim 73, further comprising presenting the information content data in the predetermined format to each requestor providing a valid key.

[c81] 81. The method of claim 80, wherein presenting the information content data comprises at least one of displaying or printing the information content data in the predetermined format.

[c82] 82. The method of claim 73, further comprising decrypting the information content data, if encrypted.

[c83] 83. The method of claim 73, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a valid key.

[c84] 84. The method of claim 73, wherein the encrypted for-

matting data and the information content data, if encrypted, are each decryptable in response to a different key.

[c85] 85. The method of claim 73, further comprising:
updating the information content data; and
formatting the updated information content data in the predetermined format based on the decrypted formatting data.

[c86] 86. The method of claim 73, further comprising encrypting the formatting data into an encrypted style sheet language transformation (SLT).

[c87] 87. The method of claim 73, further comprising encrypting the information content data into an encrypted markup language (ML).

[c88] 88. The method of claim 73, further comprising transmitting the information content data in an encrypted ML and the formatting data in an encrypted SLT to a requestor.

[c89] 89. The method of claim 73, further comprising transmitting the information content data in the predetermined format in hypertext markup language (HTML) to a requestor.

[c90] 90. A method for presentation integrity, comprising:
accessing a chosen information page via a browser;
decrypting encrypted formatting data associated with the chosen information page;
formatting the chosen information page in a predetermined format based on the formatting data; and
presenting the chosen information page in the predetermined format.

[c91] 91. The method of claim 90, further comprising preventing the chosen information page from being formatted other than in the predetermined format.

[c92] 92. The method of claim 90, further comprising presenting the chosen information page in the predetermined format to each user in response to the user entering a valid password.

[c93] 93. The method of claim 90, wherein the chosen information page is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the chosen information page in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

[c94] 94. The method of claim 90, wherein the encrypted formatting data is decryptable in response to a valid password.

[c95] 95. The method of claim 90, further comprising:
presenting any parameter options for selection by a user; and
modifying the chosen information page in response to any parameter options selected by the user.

[c96] 96. The method of claim 90, further comprising:
transforming the chosen information page from a markup language to HTML in the predetermined format based on the formatting data structure in SLT; and
transmitting the chosen information page in HTML to the browser.

[c97] 97. The method of claim 96, further comprising transmitting the selected information page from a server to a client in HTML.

[c98] 98. The method of claim 96, further comprising transmitting the selected information page from a server to a client in an encrypted ML.

[c99] 99. The method of claim 96, further comprising transmitting the formatting data structure from a server to a client in an encrypted SLT.

[c100] 100. A method for presentation integrity, comprising:
encrypting formatting data associated with information content data, wherein the information content data is presentable in a predetermined format based on the decrypted formatting data; and
transmitting the information content data and the encrypted formatting data to a requestor.

[c101] 101. The method of claim 100, further comprising preventing the associated information content data from being formatted other than in the predetermined format.

[c102] 102. The method of claim 100, further comprising sending the encrypted formatting data and the information content data to a plurality of requestors, wherein the information content data is presentable in the predetermined format at each requestor.

[c103] 103. The method of claim 100, wherein the information content data is presentable into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

[c104] 104. The method of claim 100, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assignable to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

[c105] 105. The method of claim 100, further comprising encrypting the information content data.

[c106] 106. The method of claim 100, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a valid key.

[c107] 107. The method of claim 100, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a different key.

[c108] 108. A method to control information content, comprising:
decrypting encrypted formatting data associated with information content data; and
formatting the associated information content data in one of a plurality of predetermined formats based on the

decrypted formatting data.

[c109] 109. The method of claim 108, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

[c110] 110. The method of claim 109, further comprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

[c111] 111. The method of claim 108, wherein the information content data is one of an audio, visual or combination audio-visual work.

[c112] 112. The method of claim 108, further comprising selecting one of a plurality of keys, each key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.

[c113] 113. The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to a valid key.

[c114] 114. The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to different keys.

[c115] 115. A method to deter unauthorized access, comprising:
encrypting each copy of a data structure to be embodied on an electronically-readable medium;
assigning a different key to decrypt the each copy of the data structure, wherein the data structure is decryptable only in response to the key assigned to the copy; and
electronically identifying each copy of the data structure with an authorized user.

[c116] 116. The method of claim 115, further comprising electronically marking each copy of the data structure to identify the authorized user.

[c117] 117. The method of claim 116, further comprising detecting an unauthorized user by comparing the electronic marking identifying the authorized user to a user having the copy of the data structure and the key assigned to the copy.

[c118] 118. The method of claim 115, further comprising electronically marking each copy of the data structure using one of a public key signature, steganography or water-

marking to identify the authorized user.

[c119] 119. The method of claim 115, wherein each copy of the data structure is encrypted by the same key assigned to decrypt the copy.

[c120] 120. The method of claim 115, wherein each copy of the data structure is encrypted by a different key compared to the key assigned to decrypt the copy.

[c121] 121. A method to deter unauthorized access, comprising:
encrypting formatting data associated with information content data;
providing the encrypted formatting data with each copy of the information content data embodied on an electronically-readable medium; and
assigning a different key to decrypt the formatting data of each copy of the information content data, wherein the formatting data of each copy of the information content data is decryptable only in response to the key assigned to the copy.

[c122] 122. The method of claim 121, further comprising identifying each copy of the information content data and the formatting data with an authorized user.

[c123] 123. The method of claim 122, further comprising elec-

tronically marking each copy of the information content data and the encrypted formatting data to identify the authorized user.

[c124] 124. The method of claim 123, further comprising detecting an unauthorized user by comparing the electronic marking identifying the authorized user to a user having the copy of the information content data and encrypted formatting data and the key assigned to the copy.

[c125] 125. The method of claim 122, further comprising electronically marking each copy of the information content data and the encrypted formatting data using one of a public key signature, steganography and watermarking to identify the authorized user.

[c126] 126. The method of claim 121, further comprising encrypting the information content data.

[c127] 127. The method of claim 126, wherein the formatting data and the information content data are each decryptable by the key assigned to the copy.

[c128] 128. The method of claim 126, wherein the information content data and the formatting data are each decryptable in response to different keys.

[c129] 129. The method of claim 126, wherein the information content data and the formatting data are encryptable in response to different keys and are decryptable in response to keys that are each different form the keys used to respectively encrypt the information content data and formatting data.

[c130] 130. The method of claim 121, further comprising presenting the information content data as one of an audio, visual, or combination audio-visual work in response to the key assigned to the copy.

[c131] 131. The method of claim 121, wherein the information content data is a software program and wherein the method further comprises authorizing use of the software program in response to the key assigned to the copy of the information content data.

[c132] 132. A computer-readable medium having computer-executable instructions for performing a method, comprising:
decrypting encrypted formatting data associated with information content data; and
formatting the associated information content data in a predetermined format based on the decrypted formatting data.

[c133] 133. The computer-readable medium having computer-executable instructions for performing the method of claim 132, further comprising preventing the associated information content data from being formatted other than in the predetermined format.

[c134] 134. The computer-readable medium having computer-executable instructions for performing the method of claim 132, further comprising sending the encrypted formatting data and the information content data to a plurality of clients, wherein the information content data is formatted in the predetermined format at each client.

[c135] 135. The computer-readable medium having computer-executable instructions for performing the method of claim 132, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

[c136] 136. The computer-readable medium having computer-executable instructions for performing the method of claim 135, further comprising formatting the information content data into different versions for different audi-

ences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

[c137] 137. The computer-readable medium having computer-executable instructions for performing the method of claim 132, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

[c138] 138. A computer-readable medium having computer-executable instructions for performing a method, comprising:
decrypting encrypted formatting data associated with information content data; and
formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data.

[c139] 139. The computer-readable medium having computer-executable instructions for performing the method of

claim 138, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

[c140] 140. The computer-readable medium having computer-executable instructions for performing the method of claim 139, further comprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

[c141] 141. The computer-readable medium having computer-executable instructions for performing the method of claim 139, further comprising selecting one of a plurality of keys, each key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.